Firewall e NIDS a. Illustrare brevemente (max 10 righe) la differenza tra Proxy e Firewall. Descrivere uno scenario in cui utilizzereste un proxy e motivare la risposta (max 10 righe) b. Quali aspetti architetturali vanno presi in considerazione per implementare un NIDS completo. Spiegare i componenti principali e dove posizionarli all'interno di un' architettura.

a. Un firewall è un componente avente lo scopo di controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno in base ad un determinato insieme di regole. Un firewall si occupa di bloccare le connessioni dalle reti non autorizzate, filtra i dati monitorando i pacchetti IP e lavora principalmente a livello di trasporto. Il proxy è un tipo di server che funge da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server, disaccoppiando la comunicazione tra due componenti rendendola indiretta. Il proxy è un componente che abilita la comunicazione tra il client e il server se il client è un utente legittimo, agisce come client e server nello stesso momento, può essere utilizzato per l'anonimato, per bypassare delle restrizioni e lavora principalmente a livello applicazione, inoltre il proxy è un componente che, se utilizzato insieme al firewall, fornisce fattibilità e maggiore efficienza. Un firewall deve essere usato nel caso in cui si volesse proteggere un pc da minacce e attacchi esterni, per bloccare l'accesso a contenuti indesiderati o pericolosi e per gestire e compartizzare la rete. Un proxy può essere utilizzato per l'anonimato, intercettare ed ispezionare i messaggi prima che arrivino al destinatario, per mantenere l'anonimato nella navigazione online e per accedere a servizi con limitazioni geografiche.
b. Per implementare un NIDS è necessario considerare alcuni aspetti architetturali: Innanzitutto è necessario stabilire quanti sensori installare nella rete tenendo conto del costo e della complessità di gestione e della ricchezza dei dati, poi è necessario determinare dove installarli, ad esempio un sensore posto all'esterno rileva l'intero traffico della rete e analizza una maggiore quantità di dati, mentre un sensore posto all'interno rileva solo il traffico che entra nella rete e non fornisce informazioni sugli attacchi bloccati dal firewall, infine è necessario stabilire come gestire i dati, ad esempio stabilise se usare un logging generalizzato o distribuito.

   Per ispezionare il traffico, sarà presente un sensore installato sul firewall, router o host e che ha il compito di analizzare il traffico di rete e scatenare eventi di sicurezza quando rileva qualcosa. Il sensore può inoltre interagire direttamente con l'ACL del firewall, chiedendo a quest'ultimo di compiere delle azioni come il reset della connessione TCP. Tutti i sensori comunicano con un loro gestore, il director ossia il sistema di coordinamento dei sensori stessi. Esso è in grado di costruire dei pattern e capire, in base alle attività dei sensori, se una certa serie di di eventi è riconducibile ad un certo pattern di attacco e agire quindi di conseguenza. Infine è fondamentale anche la presenza di un sistema di comunicazione dei messaggi tra i sensori, il quale deve essere sicuro e affidabile per permettere il corretto funzionamento dell'IDS. NB: quest'ultimo può essere un target degli attaccanti i quali, per prima cosa. punteranno a neutralizzarlo.

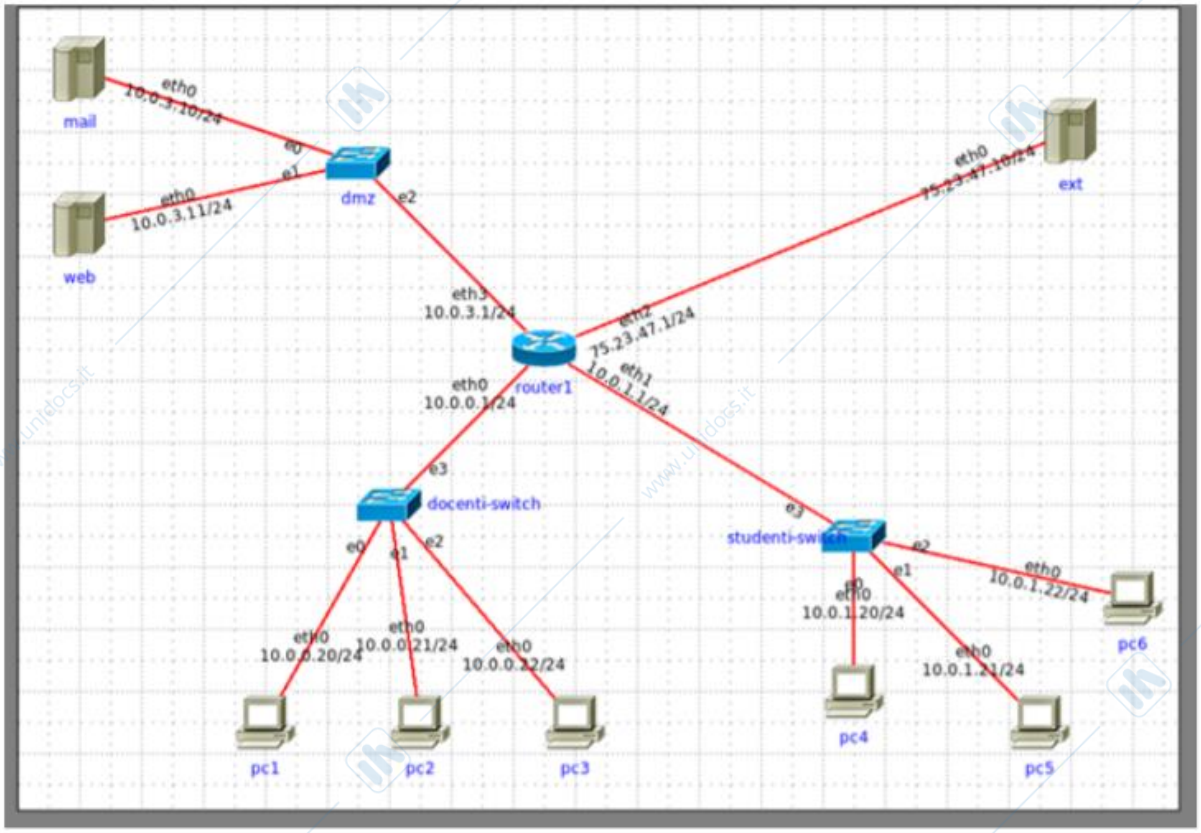
Firewall a. Consideriamo il problema di filtrare il traffico da e verso un server FTP attraverso un firewall . Usereste FTP attivo o passivo? b Sarebbe utile un IDS in tal senso o no? Motivare le risposte. c Cosa è possibile fare con uno stateful filtering che non si riesce ad ottenere con lo stateless?

a. Nel FTP passivo il server conferma la connessione e comunica la porta in cui si pone in ascolto, generalmente una porta random in un preciso range impostato lato server, per questo motivo sceglierei l' FTP passivo in quanto se ben gestito consente l'apertura e la chiusura di porte casuali, riducendo i rischi legati a possibili attacchi.

b. Uno stateless firewall analizza ogni pacchetto che lo attraversa singolarmente, senza tenere conto dei pacchetti che lo hanno preceduto. In tale analisi vengono considerate solo alcune informazioni contenute nell'header del pacchetto ovvero l'indirizzo IP della sorgente, l'indirizzo IP della destinazione, la porta della sorgente, la porta della destinazione e il protocollo di trasporto. Su questi parametri vengono costruite le regole che formalizzano la policy del firewall e che stabiliscono quali pacchetti lasciar passare e quali bloccare. Questo tipo di filtraggio è semplice e leggero ma non garantisce un'elevata sicurezza. Infatti, risulta vulnerabile ad attacchi di tipo IP spoofing in quanto non riesce a distinguere se un pacchetto appartenga o no ad una connessione attiva. Questo controllo del firewall avviene a livello di rete.

Uno stateful firewall o circuit-level gateway svolge lo stesso tipo di filtraggio dei packet filter firewall e in più tiene traccia delle connessioni e del loro stato. Questa funzionalità, detta stateful inspection, viene implementata utilizzando una tabella dello stato interna al firewall nella quale ogni connessione TCP e UDP viene rappresentata da due coppie formate da indirizzo IP e porta, una per ciascun endpoint della comunicazione. Questo controllo avviene a livello di trasporto. I firewall con stato sono un'estensione più avanzata e moderna dei firewall con filtro pacchetti senza stato in quanto sono continuamente in grado di tenere traccia dello stato della rete e delle connessioni attive che ha come flussi TCP o comunicazioni UDP.

Firewall a. Cosa si intende per IDS e per IPS, in cosa differiscono? Elencare alcuni strumenti di IDS e IPS conosciuti. Che ruolo possono assumere i firewall in relazione a sistemi IPS? Fare un esempio. b. Considerando la topologia sottostante (router 1 è il firewall, ext la rete esterna internet) dove posizionereste i sensori IDS/IPS?



a. L'IDS è un sistema per identificare individui che usano un computer o una rete senza autorizzazione, esteso anche all'identificazione di utenti autorizzati, ma che violano i loro privilegi. In generale, rileva comportamenti non conformi. L'ipotesi che sta alla base di questa definizione è che il "pattern" di comportamento degli utenti non autorizzati si differenzia da quello degli utenti autorizzati. Gli IDS vengono usati per: • rilevare attacchi o altre violazioni alla sicurezza che non sono prevenuti da altri sistemi • fornire utili informazioni su intrusioni avvenute, fare diagnosi e correzioni di eventuali debolezze • avere risposte automatiche come la chiusura di una connessione, l'aumento della sensibilità di un IDS o lo spegnimento di un host sotto attacco.
Gli IPS sono dei componenti software attivi sviluppati per segnalare e bloccare le attività dannose. Rappresentano un'estensione degli strumenti di intrusion detection system (IDS), sono posizionati inline e sono abilitati a prevenire e bloccare le intrusioni identificate. Più specificamente, IPS può eseguire alcune azioni come mandare un allarme, eliminare pacchetti malevoli, resettare le connessioni e/o bloccare il traffico da un indirizzo IP attaccante. IPS può anche correggere gli errori CRC (Cyclic redundancy check), deframmentare pacchetti, evitare problemi di sequenza TCP e ripulire i livelli di trasporto e rete da opzioni indesiderate. Gli Intrusion prevention system sono basati su una lista di controllo degli accessi simile a quella utilizzata da un firewall, con la differenza che quest'ultimo lavora a livello di trasporto e di rete su porte e indirizzi IP mentre questa tecnologia lavora a livello applicativo su programmi/servizi e utenti. L'Intrusion prevention system evita dunque l'attivazione di programmi potenzialmente malevoli.

La differenza tra i due sta nel fatto che IDS è un sistema che monitora la rete e rileva attività inappropriate, errate o anomale, mentre un IPS è un sistema che rileva l'intrusione o un attacco e prende provvedimenti attivi per prevenirli. IPS prende attivamente provvedimenti per prevenire o bloccare le intrusioni rilevate. Questi passaggi di prevenzione includono attività come la rimozione di pacchetti dannosi e il ripristino o il blocco del traffico proveniente da indirizzi IP dannosi. IPS può essere visto come un'estensione di IDS, che ha le funzionalità aggiuntive per prevenire le intrusioni durante il rilevamento.

Uno strumento IDS conosciuto è il NIDS, (network intrusion detection system), uno strumento dedito ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o probabili intrusioni informatiche. Le logiche su cui i NIDS si basano per riconoscere flussi non autorizzati si distinguono in: Pattern Matching e Anomaly Detection. Le componenti di un NIDS sono: • Sensor: – controlla traffico e log individuando pattern sospetti – attiva i security event rilevanti – interagisce con il sistema (ACLs, TCP reset, ...) • Director: – coordina i sensor – gestisce il security database • IDS message system: consente la comunicazione sicura ed affidabile tra i componenti dell'IDS.

Un honeypot (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici. Solitamente consiste in un computer o un sito che sembra essere parte della rete e contenere informazioni preziose, ma che in realtà è ben isolato e non ha contenuti sensibili o critici. Il valore primario di un honeypot è l'informazione che esso dà sulla natura e la frequenza di eventuali attacchi subiti dalla rete. Gli honeypot non contengono informazioni reali e quindi non dovrebbero essere coinvolti da nessuna attività; rilevazioni in senso opposto possono rivelare intrusioni non autorizzate o malevole in corso.

Snort è uno strumento gratuito, testato, diffuso e ben supportato. Può funzionare sia come normale sniffer, sia come IDS. Il funzionamento avviene impostando il programma in una delle sue modalità principali:
• Sniffer: il programma legge i pacchetti di rete e li mostra sulla console. Visualizza i pacchetti come un flusso continuo. Si può dire che è simile al funzionamento di tcpdump.
• Packet Logger: il programma esegue il log dei pacchetti di rete su disco. In pratica è una modalità simile a quella Sniffer ma che presenta molte più opzioni. I log dei pacchetti vengono salvati su disco.
• NIDS: il programma analizza il traffico di rete e sulla base di regole definite dall'utente (regole snort-based) scattano dei particolari allarmi.
• Inline: riceve i pacchetti direttamente da IpTables e collabora per bloccare traffico sospetto (IPS).

Gli Intrusion prevention system sono basati su una lista di controllo degli accessi simile a quella utilizzata da un firewall, con la differenza che quest'ultimo lavora a livello di trasporto e di rete su porte e indirizzi IP mentre questa tecnologia lavora a livello applicativo su programmi/servizi e utenti.

b) posizionerei almeno un sensore dotato di un ampio insieme di firme tra il firewall e la rete esterna e almeno altri tre sensori con solo un ristretto e personalizzato set di firme, posizionati rispettivamente tra dmz e router, tra docenti-switch e router e tra studenti switch e router, per coprire potenziali flussi di traffico a livello laterale.

Firewall e NIDS a. Come cooperano firewall e IPS? b. Assumendo un firewall posizionato su un router, devono essere filtrati i traffici in ingresso al firewall stesso o solo quelli che devono essere "forwarded"? Spiegare le motivazioni contestualizzando lo scenario.

a. Un IPS collabora con un firewall contribuendo con un livello aggiuntivo di protezione, in particolare un firewall si occupa di autorizzare o negare il traffico in base ad un set di regole prestabilite e costituisce la prima linea di difesa contro gli attacchi, esso di solito ha molte interfacce di rete fisiche per segmentare la rete in diverse zone di sicurezza. L'IPS è solitamente posizionato dietro al firewall, Esso si occupa dell'ispezione dei pacchetti di rete per confrontarli con i pattern degli attacchi noti. Quindi, il traffico viene bloccato o viene emesso un allarme, esso inoltre deve essere ad alte prestazioni per eseguire Deep Packet Inspection e non rallentare il traffico.
Intrusion prevention system sono basati su una lista di controllo degli accessi simile a quella utilizzata da un firewall, con la differenza che quest'ultimo lavora a livello di trasporto e di rete su porte e indirizzi IP mentre questa tecnologia lavora a livello applicativo su programmi/servizi e utenti.

E' possibile per un firewall filtrare traffico criptato? Spiegare se non è possibile perché mentre se è possibile come.?

Per un firewall risulta difficile filtrare traffico criptato, per farlo sono state proposte alcune soluzioni come quella di SonicWall che propone, attraverso il suo software, di bloccare il malware crittografato prima che entri nella rete, scansionare una vasta gamma di protocolli di crittografia e ottenere una protezione avanzata contro le ultime minacce. Infatti molte funzionalità vengono aggiunte nella fase di filtraggio (DPI)

Firewall a. Consideriamo il problema di filtrare il traffico da e verso un server FTP attraverso un firewall. Usereste FTP attivo o passivo? b. Descrivere in forma tabellare quali sarebbero le regole da implementare in un firewall facendo le opportune assunzioni sugli indirizzi e sulle reti da considerare (es. rete interna rete esterna).

c. Ammesso di aver impostato correttamente il firewall quali problemi di sicurezza permangono insiti nel protocollo FTP? Come si potrebbero risolvere?

Direz. IP Sorg IP Dest Protoc. Porta Sorg Porta Dest Flag ACK Azione

a. Per filtrare il traffico FTP attraverso un firewall userei la modalità passiva in quanto la modalità attiva crea problemi e per essere utilizzata deve essere per forza accompagnata da un packet filtering che si ricordi delle connessioni. Sarebbe quindi necessario scrivere una regola che consenta il traffico entrante iniziato dall'esterno con source port sport = 20 e destination port dport > 1023, regola pericolosa perchè vengono lasciate tutte le porte dinamiche aperte in quanto non si sa quale è la porta sulla quale il client vorrà comunicare. La modalità passiva risolve questo problema, in cui le connessioni vanno tutte dal client verso il server in modo monodirezionale. Come primo passo avviene sempre l'handshake del client sulla porta 21, dicendo al server che si vuole abilitare la modalità passiva. Vedendo tale esigenza il server non userà più la porta 20 per i dati ma indicherà al client la porta (random) sulla quale vorrà comunicare successivamente. Il client una volta ricevuta tale informazione effettuerà il 3-way handshake proprio su quella porta; questa seconda connessione, relativa al canale dati, viene aperta dal client verso il server

b.

Direz.	IP Sorg	IP Dest	Protoc.	Porta Sorg	Porta Dest	Flag ACK	Azione
OUT	Internal	External	TCP	>1023	21	1/0	Permit
IN	External	Internal	TCP	21	>1023	1	Permit
OUT	Internal	External	TCP	>1023	>1023	1/0	Permit
IN	External	Internal	TCP	>1023	>1023	1	Permit
Any	Any	Any	Any	Any	Any	**	Deny

c. I problemi caratteristici del protocollo FTP sono: Mancanza di crittografia e autenticazione: i dati inviati tramite FTP non vengono crittografati e vengono invece inviati "in chiaro", FTP è un protocollo obsoleto che non è più aggiornato e di conseguenza non è scalabile, FTP non soddisfa i requisiti di conformità, molti regolamenti richiedono degli standard di sicurezza minimi che le organizzazioni dovrebbero adottare e FTP non è tra questi. Una soluzione per ovviare a questi problemi potrebbe essere ad esempio l'uso di FTPS, overo un protocollo nato da FTP che usa un sotto strato SSL/TLS che permette di crittare i dati in transito. Un'altra soluzione consiste nell'abbandonare FTP ed utilizzare protocolli più sicuri ed aggiornati che prevedano l'utilizzo della crittografia e dell'autenticazione a più fattori.

Che differenza esiste tra static e dynamic packet filtering nei firewall? Fare degli esempi.

Lo static filtering valuta ogni pacchetto indipendentemente, senza alcun riferimento a eventuali pacchetti precedenti, ha delle regole predefinite, che permettono di bloccare solo gli attacchi più banali per la sicurezza interna delle reti e per avere una prima schermatura; hanno ovviamente il problema che non analizzano il payload, dove potrebbero nascondersi ulteriori attacchi. Nel dynamic filter la decisione se passare un pacchetto dipende da quali pacchetti sono già passati attraverso il firewall. I dynamic filter inoltre aprono i pacchetti, introducendo ovviamente della latenza, problemi di performance e costi più elevati. Inoltre sono in grado di capire lo stato analizzando il livello di trasporto e/o quello applicativo, cercando così di dare un senso ai protocolli di livello superiore e adattando le regole di filtraggio di conseguenza. Sono in grado anche di distinguere le nuove connessioni da quelle già aperte mantenendo delle tabelle di stato in memoria in cui si tiene traccia delle sessioni. Hanno delle prestazioni dal punto di vista della sicurezza migliori, anche se presentano delle limitazioni in alcuni scenari dove le applicazioni sono complicate.

Come vengono gestite le comunicazioni TCP in un firewall stateful? E le connessioni UDP?

Per gestire le comunicazioni TCP vengono ovviamente definite delle regole, in particolare ciò avviene mediante l'ispezione dei tentativi di connessione e verranno scritte solo quelle relative all'apertura delle connessioni TCP (guardando il SYN). Non serve infatti specificare le regole per le risposte come nel packet filter, in quanto gestite automaticamente controllando la connection table.

Il problema sorge con i protocolli non orientati alla connessione e che non possiedono quindi informazioni di stato, i cosiddetti protocolli connectionless come UDP. In questo caso viene gestito uno pseudo-stato ottenuto correlando semplicemente indirizzi IP e porte (sorgente e destinazione). In questo modo viene costruita una tabella che viene utilizzata per gestire questi protocolli connectionless; in questo caso non ci sarà alcun flag FIN e quindi risulterà fondamentale il timeout.

Con IPTABLES è possibile gestire lo stato delle connessioni? Come?

La gestione dello stato delle connessioni è fatta richiamando il modulo di match state che permette di dividere il traffico secondo diversi stati:
NEW - Il primo pacchetto relativo ad una nuova connessione (syn TCP o nuovo pacchetto UPD)
ESTABLISHED - Pacchetti relativi a connessioni già stabilite, in cui si è avuto almeno un pacchetto da entrambi i peer
RELATED - Pacchetti in qualche modo correlati a connessioni esistenti ed established. Ticipi esempi il traffico di dati FTP o il trasferimetno DCC in IRC.
INVALID - Pacchetti che non rientrano in alcuno dei suddetti stati, di solito vengono droppati.

Spiegare cosa sono le catene di filtraggio in un firewall IPTABLES. Quante sono? Illustrare un esempio di una catena personalizzata

Le catene di filtraggio rappresentano un insieme di regole su cui si basa il sistema netfliter, le catene a loro volta raggruppate in tabelle. Ogni tabella definisce un tipo diverso di operazioni che è possibile effettuare sui pacchetti; ogni catena definisce come vengono trattati i pacchetti nelle diverse fasi della loro elaborazione. Le catene rappresentano una forma di lista di controllo degli accessi (ACL): ogni regola è costituita da due parti: le caratteristiche che un pacchetto deve avere affinché la regola stessa venga applicata e un obiettivo o target, che indica cosa fare quando il pacchetto rispetta le caratteristiche indicate. A ciascuna catena è anche associata una politica di default, che definisce come vengono trattati i pacchetti che non corrispondono ad alcuna regola.

Esistono 5 tipi di catene: INPUT, OUTPUT, FORWARD, PREROUTING e POSTROUTING:

- **INPUT**: Si lavora sui **pacchetti in entrata** nel sistema
- **OTPUT**: Si lavora sui **pacchetti in uscita** dal sistema
- **FORWARD**: Si lavora sui **pacchetti che sono diretti ad un altro host della rete ma che per poterci arrivare devono passare dal nostro sistema**: in pratica il sistema agisce come un router

- **PREROUTING**: Si lavora sui pacchetti in entrata ma **a questi pacchetti vengono già applicate delle regole ben definite prima di essere instradate nel sistema.**
- **POSTROUTING**: Si lavora sui **pacchetti in uscita dal sistema ma solamente dopo che è stato deciso il loro instradamento**

Esempio catena

iptables -N catenapersonalizz

iptables -P catenapersonalizz -j DROP

iptables -A catenapersonalizz -p tcp –dport 8080 -s IP-PC3 -j ACCEPT

iptables -A catenapersonalizz -p tcp –sport 8080 -d IP-PC3 -j ACCEPT

Illustrare brevemente le principali funzionalità di un Proxy (max 10 righe). Quali sono i vantaggi rispetto un firewall stateful?

Un proxy è un componente che media le comunicazioni tra altri due componenti e che è in grado di guardare all'interno dei pacchetti: disaccoppiano quindi la comunicazione tra due componenti, rendendola indiretta. Inoltre, essendo che i dati transitando nella rete vengono in un certo senso "spezzati", il proxy deve essere in grado di ricostruire ciò che arriva nell'ordine corretto.

Le principali tipologie di proxy sono:

● web proxy, si occupano principalmente del caching di pagine web. Dopo una serie di richieste ad una certa pagina questa verrà salvata appunto nella cache e alla prossima richiesta sarà proprio il proxy a rispondere, migliorando così le performance;

● anonymizing proxy, si occupano dell'anonimizzazione di connessioni web. La tipologia distorting fa in modo che l'IP non sia rintracciabile, mentre gli high anonymity proxy servers non si limitano ad anonimizzare solo l'IP ma anche aspetti più avanzati;

● reverse proxy, garantiscono l'accesso da utenti esterni a risorse interne;

● proxy firewall, mediano connessioni applicative e gestiscono aspetti di sicurezza dei protocolli.

Differenza tra statefull firewall e application gateway

Uno statefull firewall analizza ogni pacchetto che lo attraversa singolarmente e in più tiene traccia delle connessioni e del loro stato, questa funzionalità, detta stateful inspection, viene implementata utilizzando una tabella dello stato interna al firewall nella quale ogni connessione TCP e UDP viene rappresentata da due coppie formate da indirizzo IP e porta, una per ciascun endpoint della comunicazione. Un application firewall o proxy firewall opera fino al livello 7 del modello OSI filtrando tutto il traffico di una singola applicazione sulla base della conoscenza del suo protocollo. Questo tipo di firewall analizza i pacchetti nella sua interezza considerando anche il loro contenuto (payload) ed è quindi in grado di distinguere il traffico di un'applicazione indipendentemente dalla porta di comunicazione che questa utilizza. Un'altra caratteristica che lo distingue da un packet filter firewall e da uno circuit firewall è la capacità di spezzare la connessione tra un host della rete che protegge e un host della rete esterna. Infatti, nelle comunicazioni svolge il ruolo di intermediario ed è quindi l'unico punto della rete che comunica con l'esterno, nascondendo così gli altri host che vi appartengono.