**Securitatea punctului final**

**Atacurile de rețea astăzi**

Presa de știri acoperă în mod obișnuit atacurile asupra rețelelor întreprinderilor. Pur și simplu căutați pe internet „cele mai recente atacuri de rețea” pentru a găsi informații actualizate despre atacurile curente. Cel mai probabil, aceste atacuri vor implica unul sau mai multe dintre următoarele:

* **Distributed Denial of Service (DDoS)** – Acesta este un atac coordonat de la multe dispozitive, numite zombi, cu intenția de a degrada sau opri accesul public la site-ul web și resursele unei organizații.
* **Încălcarea datelor** – Acesta este un atac în care serverele de date sau gazdele unei organizații sunt compromise pentru a fura informații confidențiale.
* **Malware** – Acesta este un atac în care gazdele unei organizații sunt infectate cu software rău intenționat care cauzează o varietate de probleme. De exemplu, ransomware precum WannaCry, prezentat în figură, criptează datele de pe o gazdă și blochează accesul la acestea până când se plătește o răscumpărare.



**Dispozitive de securitate de rețea**

Sunt necesare diverse dispozitive de securitate pentru a proteja perimetrul rețelei de accesul din exterior. Aceste dispozitive ar putea include un router activat pentru rețea privată virtuală (VPN), un firewall de ultimă generație (NGFW) și un dispozitiv de control al accesului la rețea (NAC).

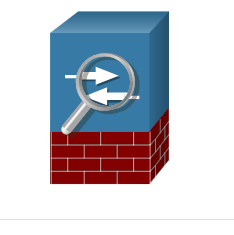
Router activat pentru VPN

Un router compatibil VPN oferă o conexiune sigură utilizatorilor la distanță printr-o rețea publică și în rețeaua întreprinderii. Serviciile VPN pot fi integrate în firewall.



**NGFW**

Un NGFW oferă inspecție completă a pachetelor, vizibilitate și control al aplicațiilor, un sistem de prevenire a intruziunilor de ultimă generație (NGIPS), protecție avansată împotriva programelor malware (AMP) și filtrare URL.



**NAC**

Un dispozitiv NAC include servicii de autentificare, autorizare și contabilitate (AAA). În întreprinderile mai mari, aceste servicii pot fi încorporate într-un dispozitiv care poate gestiona politicile de acces pentru o mare varietate de utilizatori și tipuri de dispozitive. Cisco Identity Services Engine (ISE) este un exemplu de dispozitiv NAC.



**Protecția punctelor finale**

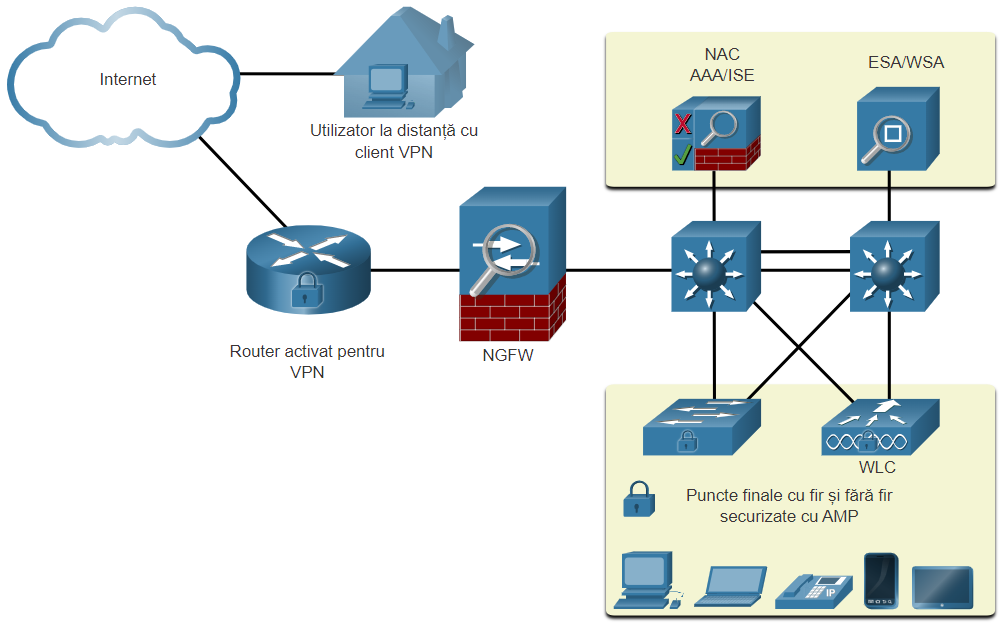
Dispozitivele LAN, cum ar fi comutatoarele, controlerele LAN fără fir (WLC) și alte dispozitive punct de acces (AP) interconectează punctele finale. Cele mai multe dintre aceste dispozitive sunt susceptibile la atacurile legate de LAN care sunt acoperite în acest modul.

Dar multe atacuri pot proveni și din interiorul rețelei. Dacă o gazdă internă este infiltrată, aceasta poate deveni un punct de plecare pentru ca un actor de amenințare să obțină acces la dispozitivele critice ale sistemului, cum ar fi serverele și datele sensibile.

Punctele finale sunt gazde care constau în mod obișnuit din laptopuri, desktop-uri, servere și telefoane IP, precum și dispozitive deținute de angajați, care sunt denumite în mod obișnuit ca dispozitive proprii (BYOD). Punctele finale sunt deosebit de susceptibile la atacuri legate de malware care provin prin e-mail sau navigare pe web. Aceste puncte finale au folosit de obicei caracteristici tradiționale de securitate bazate pe gazdă, cum ar fi antivirus/antimalware, firewall-uri bazate pe gazdă și sisteme de prevenire a intruziunilor (HIPS) bazate pe gazdă. Cu toate acestea, punctele finale de astăzi sunt cel mai bine protejate printr-o combinație de NAC, software AMP bazat pe gazdă, un dispozitiv de securitate pentru e-mail (ESA) și un dispozitiv de securitate web (WSA). Produsele Advanced Malware Protection (AMP) includ soluții pentru puncte finale, cum ar fi Cisco AMP pentru puncte finale.

Figura este o topologie simplă reprezentând toate dispozitivele de securitate ale rețelei și soluțiile pentru punctele finale discutate în acest modul.

Figura este o topologie de rețea care arată dispozitivele de securitate ale rețelei și soluțiile terminale. În stânga sus este cloud-ul Internet. Atașat la cloud-ul Internet este un utilizator de la distanță cu client VPN. Conectat la cloud din rețeaua internă este un router compatibil VPN care este conectat la un NGFW. NGFW este conectat la un comutator multistrat care are două conexiuni la un alt comutator multistrat. Conectat la primul comutator este un dispozitiv NAC AAA/ISE. Conectat la al doilea comutator este un dispozitiv ESA/WSA. Cele două comutatoare multistrat sunt ambele conectate la un comutator LAN securizat și la un WLC. Sunt afișate, de asemenea, mai multe puncte finale cu fir și fără fir securizate cu AMP, inclusiv un desktop, laptop, telefon IP și smartphone.

**Dispozitivul Cisco Email Security**

Dispozitivele de securitate a conținutului includ un control fin asupra e-mailului și a navigării pe web pentru utilizatorii unei organizații.

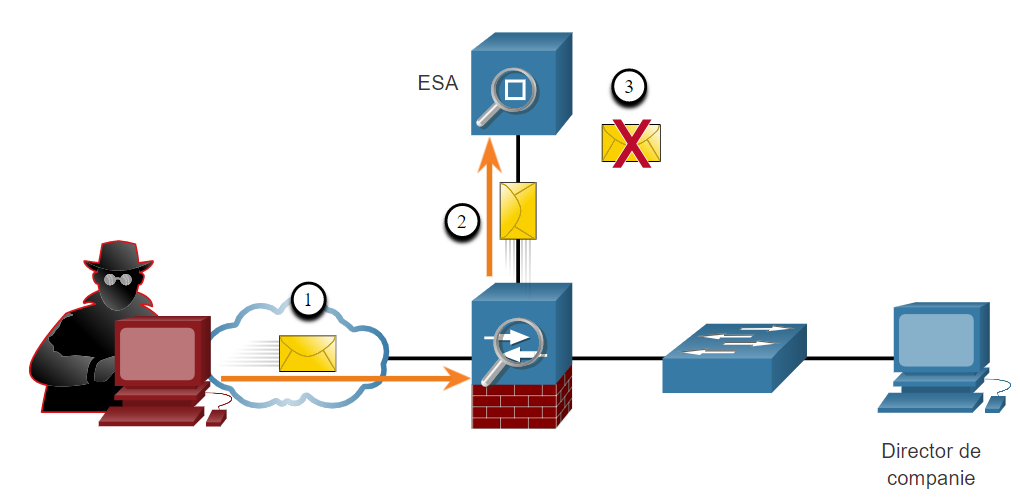
Potrivit Cisco's Talos Intelligence Group, în iunie 2019, 85% din toate e-mailurile trimise erau spam. Atacurile de tip phishing sunt o formă deosebit de virulentă de spam. Amintiți-vă că un atac de tip phishing atrage utilizatorul să facă clic pe un link sau să deschidă un atașament. Spear phishing vizează angajații sau directorii de rang înalt care ar putea avea acreditări de conectare ridicate. Acest lucru este deosebit de crucial în mediul actual în care, potrivit Institutului SANS, 95% din toate atacurile asupra rețelelor întreprinderilor sunt rezultatul unui atac de tip spear phishing de succes.

Cisco ESA este un dispozitiv conceput pentru a monitoriza protocolul SMTP (Simple Mail Transfer Protocol). Cisco ESA este actualizat constant prin fluxuri în timp real de la Cisco Talos, care detectează și corelează amenințările și soluțiile prin utilizarea unui sistem de monitorizare a bazelor de date la nivel mondial. Aceste date de informații despre amenințări sunt extrase de Cisco ESA la fiecare trei până la cinci minute. Acestea sunt câteva dintre funcțiile Cisco ESA:

* Blocați amenințările cunoscute.
* Remediați malware-ul ascuns care s-a susținut de la detectarea inițială.
* Aruncă e-mailurile cu linkuri greșite (după cum se arată în figură).
* Blocați accesul la site-urile nou infectate.
* Criptați conținutul din e-mailurile trimise pentru a preveni pierderea datelor.

În figură, Cisco ESA renunță la e-mailul cu link-uri proaste.

un actor de amenințare trimite un e-mail de phishing din cloud destinat unui director de companie; firewall-ul îl transmite către ESA care îl renunță



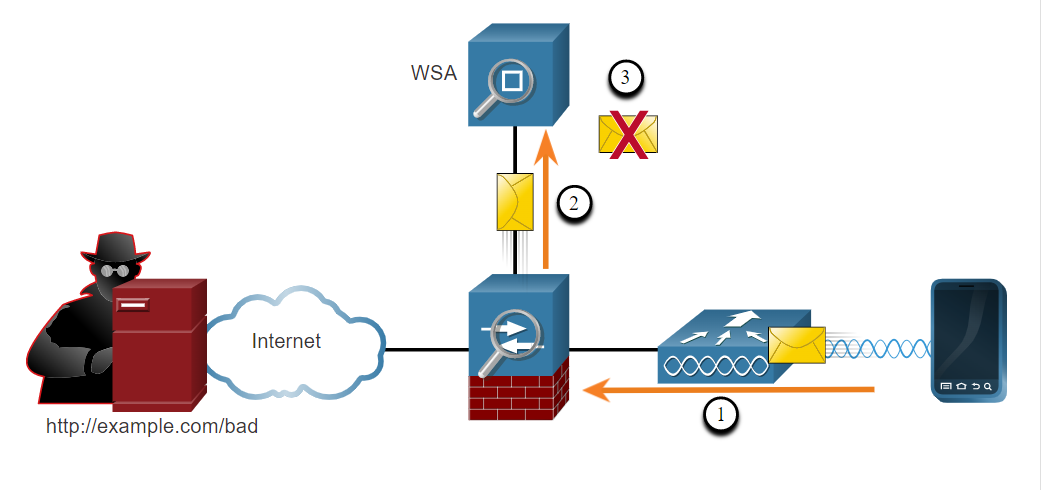
1. Agentul de amenințare trimite un atac de tip phishing către o gazdă importantă din rețea.
2. Firewall-ul redirecționează toate e-mailurile către ESA.
3. ESA analizează e-mailul, îl înregistrează și, dacă este un malware, îl aruncă.

**Cisco Web Security Appliance**

Cisco Web Security Appliance (WSA) este o tehnologie de atenuare a amenințărilor bazate pe web. Ajută organizațiile să facă față provocărilor legate de securizarea și controlul traficului web. Cisco WSA combină protecția avansată împotriva programelor malware, vizibilitatea și controlul aplicațiilor, controalele privind politica de utilizare acceptabilă și raportarea.

Cisco WSA oferă control complet asupra modului în care utilizatorii accesează internetul. Anumite funcții și aplicații, cum ar fi chat, mesagerie, video și audio, pot fi permise, restricționate cu limite de timp și lățime de bandă sau blocate, în funcție de cerințele organizației. WSA poate efectua lista neagră a adreselor URL, filtrarea URL-urilor, scanarea programelor malware, clasificarea URL-urilor, filtrarea aplicațiilor web și criptarea și decriptarea traficului web.

În figură, un angajat intern al companiei folosește un smartphone pentru a încerca să se conecteze la un site cunoscut pe lista neagră.



1. Un utilizator încearcă să se conecteze la un site web.
2. Firewall-ul transmite solicitarea site-ului către WSA.
3. WSA evaluează adresa URL și determină că este un site cunoscut pe lista neagră. WSA renunță la pachet și trimite utilizatorului un mesaj de acces refuzat.